

REMARKS

The following Request for Reconsideration is submitted in response to the Office Action issued on October 12, 2003 (Paper No. unknown) in connection with the above-identified patent application, and is being filed within the three-month shortened statutory period set for a response by the Office Action.

Claims 1-46 remain pending in the present application, and stand rejected. Applicants again respectfully request reconsideration and withdrawal of the rejection of the claims, consistent with the following remarks.

Applicants note that in response to the Appeal Brief filed on July 12, 2004 in connection with the above-identified matter, the Examiner has chosen to withdraw the rejection that was the basis for appeal and has reopened prosecution to assert a new rejection. In particular, the Examiner has now rejected claims 1-46 under 35 USC § 102 as being anticipated by Minear et al. (U.S. Patent No. 5,983,350). Applicants respectfully traverse the § 102 rejection of such claims.

As was previously pointed out, independent claim 1 recites a method for releasing digital content to a rendering application, where the rendering application forwards the digital content to an ultimate destination by way of a path therebetween. Significantly, the path is defined by at least one module and the digital content is initially in an encrypted form.

In the method, an authentication of at least a portion of the path is performed to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. If in fact each such defining module is to be trusted based on the authentication, the encrypted digital content is decrypted and forwarded to the

rendering application for further forwarding to the ultimate destination by way of the authenticated path.

Independent claim 24 recites substantially the same subject matter as claim 1, albeit as a computer-readable medium having computer-executable instructions thereon that perform the method.

Once again, with the present invention, encrypted content is decrypted and released to a rendering application only after an authentication determines that trust may be imparted to the path that the rendering application will employ to forward the decrypted content to the ultimate destination. To again summarize, then, the present invention requires –

- (1) a rendering application forwarding digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module;
- (2) an authentication of the path; and
- (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

The rendering application may be any application that renders content, such as an audio player rendering audio from audio content, a video player rendering video from video content, a visual renderer rendering a picture from picture content, or the like. Significantly, the path is not merely a wire or a communications channel, but is defined by interconnected modules, such as for example audio filters, video filters, picture filters, and the like.

Also significantly, inasmuch as the content passing through the modules / filters that define the path is to be decrypted content, such modules / filters of the path must

be trusted to handle the decrypted content in a trusted manner, and are therefore each authenticated to determine trustworthiness. Such trust is for example with regard to the fact that the modules / filters defining the path will not copy the decrypted content for nefarious purposes.

As may be appreciated, in the course of being authenticated, a particular module may prove its trustworthiness by, for example, proffering a digital certificate issued by an entity that may itself be deemed to be trustworthy. Thus, and again, the present invention is especially useful when the encrypted content is of a type that should not be copied in a decrypted form, such as for example copyright-protected audio and/or video and/or picture content.

The Minear reference discloses a method and mechanism by which a message is received over the Internet, particularly where the message has been encrypted by the sender according to a particular IPSEC standard. As best set forth at column 5, line 34 through column 6, line 26, the message is received over an unprotected network 16 by a firewall 18 of a workstation 20 and accordingly is in the encrypted form. As the message passes through a network protocol stack 40 of the workstation 20, it is determined that the message is encrypted and therefore such message is decrypted (column 6, lines 9-13) and forwarded through the stack 40 for further processing, including authentication of the sender (column 6, lines 13-18). The Minear reference also speaks of authenticating sent packets (column 3, lines 64-66) and authenticated communications session between a sending and receiving firewall (column 4, lines 37-42).

Significantly, although the Minear reference speaks of authenticating in at least the three instances set forth above, such Minear reference is entirely silent regarding any

authentication of the path through which the decrypted message flows. Accordingly, the Minear reference does not at all disclose authenticating a path through which decrypted content is forwarded, as is required by claims 1 and 24. As may be appreciated, in the Minear reference such path would include that part of the stack 40 after the message has been decrypted. As may also be appreciated, such path would not include the Internet inasmuch as the Minear message within such Internet is disclosed as being encrypted.

Moreover, and at any rate, the Minear reference clearly discloses that the decrypting of the message takes place before authentication of same. Accordingly, such Minear reference cannot be said to disclose a decryption and forwarding of decrypted content through a path, but only if an authentication (performed prior to such decryption) succeeds, as is also required by claims 1 and 24. As should be understood, it makes little sense to decrypt content to be sent down an exposed path if the path is not first authenticated, especially if a failure of the path to authenticate would obviate the need for such decryption.

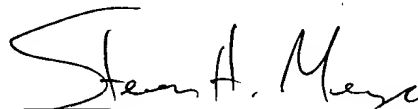
Thus, for the aforementioned reasons, Applicants respectfully submit that the Minear reference cannot be applied to anticipate the subject matter recited in claims 1 or 24, or any claims depending therefrom, including claims 2-23 and 25-46. Thus, Applicants respectfully request reconsideration and withdrawal of the § 102 rejection.

DOCKET NO.: MSFT-0135/147325.1
Application No.: 09/525,510
Office Action Dated: October 12, 2004

PATENT

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 1-46, is in condition for allowance, and such action is respectfully requested.

Respectfully Submitted

A handwritten signature in dark ink, appearing to read "Steven H. Meyer", is written over a horizontal line.

Steven H. Meyer
Registration No. 37,189

Date: January 7, 2005

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439